



## **APPLICANT RESPONSE TO FINAL OFFICE ACTION**

### **AMENDMENT AFTER FINAL**

Inventor Nick Nassiri (hereinafter referred to as the "Applicant") is in receipt of the Examiner's Action dated February 16, 2006 with respect to the above referenced patent application. Applicant wishes to address each of the Examiner's objections as put forth in the Final Office Action.

### **SPECIFICATION**

Applicant agrees with Examiner that the substitute specification is rife with deletions; however, Applicant submits that deletions do not constitute new matter. Having said that, Applicant has amended the portions of the specification wherein the Examiner states the specification constitutes new matter.

Specifically, in page 4 of the Office Action, Examiner states that:

- (i) Page 4, paragraph 3, Examiner states that replacement paragraphs 16-20 has added live stream methods and that the use of the term "authentication" as opposed to "authentication" which are not supported by the original disclosure;
- (ii) Page 4, paragraph 4, Examiner states that replacement paragraphs 62-64 have significantly changed the brief descriptions of the original

drawings and added references that did not exist in the original disclosure;

- (iii) Page 4, paragraph 5, Examiner states that replacement paragraphs 178-184 that Applicant has deleted or changed several term definitions that affect the remainder of the disclosure.

With reference to the foregoing objections cited by the Examiner, Applicant elects to cancel what the Examiner cites as new matter in replacement paragraphs 16-20. Accordingly, Applicant has revised the substitute specification in accordance with the guidelines of CFR § 1.121 (b).<sup>1</sup>

---

<sup>1</sup> Specification. Amendments to the specification, other than the claims, computer listings (§ 1.96) and sequence listings (§ 1.825), must be made by adding, deleting or replacing a paragraph, by replacing a section, or by a substitute specification, in the manner specified in this section.

(1) Amendment to delete, replace, or add a paragraph. Amendments to the specification, including amendment to a section heading or the title of the invention which are considered for amendment purposes to be an amendment of a paragraph, must be made by submitting:

(i) An instruction, which unambiguously identifies the location, to delete one or more paragraphs of the specification, replace a paragraph with one or more replacement paragraphs, or add one or more paragraphs;

(ii) The full text of any replacement paragraph with markings to show all the changes relative to the previous version of the paragraph. The text of any added subject matter must be shown by underlining the added text. The text of any deleted matter must be shown by strike-through except that double brackets placed before and after the deleted characters may be used to show deletion of five or fewer consecutive characters. The text of any deleted subject matter must be shown by being placed within double brackets if strike-through cannot be easily perceived;

Application Number 09/973, 273

Applicant respectfully submits the revised substitute specification comports with CFR § 1.121 (b)); clearly identifying the deletions and revisions for the Examiner's review vis-à-vis the original specification.

---

(iii) The full text of any added paragraphs without any underlining; and

(iv) The text of a paragraph to be deleted must not be presented with strike-through or placed within double brackets. The instruction to delete may identify a paragraph by its paragraph number or include a few words from the beginning, and end, of the paragraph, if needed for paragraph identification purposes.

(2) Amendment by replacement section. If the sections of the specification contain section headings as provided in § 1.77(b), § 1.154(b), or § 1.163(c), amendments to the specification, other than the claims, may be made by submitting:

(i) A reference to the section heading along with an instruction, which unambiguously identifies the location, to delete that section of the specification and to replace such deleted section with a replacement section; and

(ii) A replacement section with markings to show all changes relative to the previous version of the section. The text of any added subject matter must be shown by underlining the added text. The text of any deleted matter must be shown by strike-through except that double brackets placed before and after the deleted characters may be used to show deletion of five or fewer consecutive characters. The text of any deleted subject matter must be shown by being placed within double brackets if strike-through cannot be easily perceived.

(3) Amendment by substitute specification. The specification, other than the claims, may also be amended by submitting:

(i) An instruction to replace the specification; and

(ii) A substitute specification in compliance with § 1.125(b) and (c).

(4) Reinstatement of previously deleted paragraph or section. A previously deleted paragraph or section may be reinstated only by a subsequent amendment adding the previously deleted paragraph or section.

## **INSTRUCTIONS FOR AMENDMENT OF THE SUBSTITUTE SPECIFICATION**

Applicant respectfully requests that the enclosed amended portions replace the existing substitute specification on file and replace the substitute specification on file where cited.

1. Per the Examiner's objection (page 4, paragraph 3 of the final office action) Applicant requests that paragraphs 16-20 of the substitute specification be deleted in their entirety and replaced with the following text:

The main problem with conventional real-time videoconferencing methods is that none of the existing systems or applications incorporate a system, method or process, whereby an identity, or a signature, or the contents of a document is authenticated during the videoconference.

Another problem with conventional real-time videoconferencing methods is that none of the existing systems or applications incorporate a system, method or process whereby biometric data is input during the videoconference to authenticate an identity, or a

signature, or the contents of a document.

Another problem with conventional real-time videoconferencing methods is that none of the existing systems or applications incorporate a system, method or process whereby a signature may be notarized by a notary public during the videoconference.

Another problem with conventional real-time videoconferencing methods is that none of the existing systems or applications incorporate a system, method or process whereby a client may tender a service request for videoconference authentication from a remote location using the Internet.

Another problem with conventional real-time videoconferencing methods is that none of the existing systems or applications incorporate a system, method or process whereby an authoritative document is created and issued during the videoconference.

Per the foregoing, Applicant has amended paragraphs 16-20 in accordance with the Examiner's objections put forth in the final office action. Nonetheless, Applicant respectfully disagrees with the Examiner's position that the last three paragraphs of 16-20 are not supported by the original disclosure. Specifically, with respect to the last three paragraphs (paragraphs 18-20) Examiner has

Application Number 09/973, 273

objected to in the amended specification as not being supported by the original specification, Applicant traverses and refers to the original disclosure:

#### PARAGRAPH 18

Paragraph 18 (as amended herein) reads: Another problem with conventional real-time videoconferencing methods is that none of the existing systems or applications incorporate a system, method or process whereby a signature may be notarized by a notary public during the videoconference.

Examiner submits that the original disclosure does not disclose use of a notary public. Applicant respectfully traverses. Support for paragraph 18 from the original disclosure:

#### CLAIMS IN SUPPORT OF PARAGRAPH 18

Applicant respectfully refers Examiner to claims 1, 17, 18, 19, 24, 40, 41, 42, 68, 69 and 70 of the original disclosure which read as follow:

1. A method and system for performing identity and signature and document authentication using a videoconference; said method and system comprising: a host computer server, a multi-point and multi-media video conference system (including fixed and portable structures), an electronic signature capture device, an electronic document, an electronic document repository,

a digital certificate, an electronic notary seal device, a biometric data capture device, and a video verification service center (VVSC); said method and system comprising the steps of: said VVSC establishing connectivity between geographically remote parties; said connectivity comprising a videoconference that broadcasts electronic data between said parties using said multi-point and multi-media video conference system; said parties viewing one another from said multi-point and multi-media video conference system; said VVSC downloading said electronic document from said host computer server; said parties viewing the same said electronic document from said multi-point and multi-media video conference system; said parties inputting an electronic signature using said electronic signature capture device; said host computer server affixing said electronic signature to said electronic document; said parties inputting biometric data using said electronic biometric data capture device; said host computer server affixing said biometric data to said electronic document; said parties inputting said digital certificate; said host computer server affixing said digital certificate to said electronic document; said electronic notary seal device inputting an electronic notary seal; said host computer server affixing said electronic notary seal to said electronic document; said host computer server encrypting said electronic document; said host computer server uploading said

electronic document to said host computer server; and said VVSC disseminating said electronic document to said parties.

17. The method of claim 1 whereby said host computer server further comprises the means whereby said electronic notary seal device inputs said electronic notary seal.

18. The system of claim 17 whereby said electronic notary seal may be in the form of a graphical representation or in the form of source code.

19. The method of claim 1 whereby said host computer server further comprises the means to affix said electronic notary seal to said electronic document.

24. A method and system for performing identity and signature and document authentication using a videoconference; said method and system comprising: a host computer server, a multi-point and multi-media video conference system (including fixed and portable structures), an electronic signature capture device, an electronic document, an electronic document repository, a digital certificate, an electronic notary seal device, a biometric data capture device, and a video verification service center (VVSC); said method and



system comprising the steps of: said VVSC establishing connectivity between geographically remote parties; said connectivity comprising a videoconference that broadcasts electronic data between said parties using said multi-point and multi-media video conference system; said parties viewing one another from said multi-point and multi-media video conference system; said VVSC downloading said electronic document from said host computer server; said parties viewing the same said electronic document from said multi-point and multi-media video conference system; said parties inputting an electronic signature using said electronic signature capture device; said host computer server affixing said electronic signature to said electronic document; said parties inputting biometric data using said electronic biometric data capture device; said host computer server affixing said biometric data to said electronic document; said parties inputting said digital certificate; said host computer server affixing said digital certificate to said electronic document; said host computer server encrypting said electronic document; said host computer server uploading said electronic document to said host computer server or to a remote server of said parties; said host computer server creating an identity-based document with said electronic document; and said host computer server disseminating said identity-based document to authorized said parties.

40. The method of claim 24 whereby said host computer server further comprises the means whereby said electronic notary seal device inputs said electronic notary seal.

41. The system of claim 40 whereby said electronic notary seal may be in the form of a graphical representation or in the form of source code.

42. The method of claim 24 whereby said host computer server further comprises the means to affix said electronic notary seal to said electronic document.

68. The method of claim 51 whereby said host computer server further comprises the means whereby said electronic notary seal device inputs said electronic notary seal.

69. The method of claim 51 whereby said electronic notary seal may be in the form of a graphical representation or in the form of source code.

70. The method of claim 51 whereby said host computer server further comprises the means to affix said electronic notary seal to

said electronic document.

ORIGINAL DISCLOSURE IN SUPPORT OF PARAGRAPH 18

Applicant respectfully further refers Examiner to paragraphs 30, 42, 43, 52, 73, 74, 80, 81, 82, 83, 84, 104, 105, 164 and 180 of the original disclosure.

[0030] In any of the embodiments of the present invention, irrespective of the type of service request, whether it be an executed, notarized electronic document or an authenticated identification card, electronic data input by the parties participating in the videoconference may be input singularly or simultaneously. Likewise, input data may comprise various forms of electronic data in a single session, such as: an electronic document, a digital certificate, an electronic notary seal, biometric data, a password or a code, a photographic image and other such data input. Any data input from any party to the videoconference is transmitted via a real time, live stream during the course of the videoconference. Any data input from any party to the videoconference that is transmitted during the course of the videoconference, may be transmitted either singularly or simultaneously by the parties. The input data is subsequently fused to an electronic document and issued to the authorized party.

[0042] (xi) a device to create an electronic notary seal (detailed in USPTO patent-pending application, identified as Customer 021907);

[0043] (xii) the means to authenticate an electronic notary seal (detailed in USPTO patent-pending application, identified as Customer 021907);

[0052] Another object of the present invention is to provide a method of identity, signature, and electronic document authentication using a real time, live stream videoconference platform that can electronically notarize electronic documents.

[0073] To put the system and method of the present invention into context of a specific transaction: two parties that are geographically remote must each individually sign a single document and have each of their respective signatures notarized by a notary public. Each party goes to an independent VVSC that is conveniently located in proximity with their physical location. The VVSC initiates a videoconference with all of the parties to the transaction, including a notary public. The videoconference comprises screens or monitors at each location whereby the parties can input and receive audio, visual and electronic data simultaneously, albeit independently at each location.

[0074] Upon initiation of the videoconference, VVSC downloads the electronic document to a central host computer that is to be signed by the parties and that is to be notarized by the notary public. The

electronic document to be downloaded may be provided in a portable format, such as a diskette or compact disc and is provided by one of the parties to the transaction. Alternatively, the electronic document may be downloaded from a repository of electronic documents maintained by the present invention.

[0080] Should notarization be required a notary public authenticates the document by verifying the identity of the signing parties and by affixing an electronic notary seal.

[0081] The notary public may be an employee who is physically located at the VVSC or may be a remote party enjoined by the videoconference. Electronic notarization parallels the customary legal form of notarization. The notary public shall require that the signatories provide such authentication information as required by law, typically a government issued photo identification card and a biometric submission, such as a signature or a thumbprint. VVSC employee notary public will have the means to verify hard copy personal identification, such as a drivers license information and to input said information electronically in the form of a source code. Likewise, VVSC employee notary public will have the means to verify the electronic signature of the party and to input said information electronically in the form of a source code. Per the methodology above, the input information is displayed on the screen or monitor as a separate

dual image.

[0082] Upon input of the personal verification information, VVSC notary public affixes an electronic notary seal to the electronic document. In the preferred embodiment of the present invention, the electronic notary seal is in the form of a graphical representation of the notary public's seal. The graphical representation is affixed to the electronic document as a visual image. Alternatively, the notary seal may be affixed to the document in the form of a source code. Any changes to the electronic document will invalidate the notary public's seal.

[0083] Upon affixing all of the required authentication information, including, but not limited to, an electronic signature, a photographic image, biometric information, source code, an electronic notary seal, a time and date stamp is applied and the electronic document is encrypted.

[0084] The signed, notarized electronic document is disseminated to the requesting party or parties. If the parties so desire, the VVSC shall archive a copy of the electronic document for future reference.

[0104] Per the method of the preferred embodiment, the webconference is capable of providing electronic notarization services to the parties. The notary public may be an employee who is physically located at the VVSC or may be a remote party enjoined by the webconference. Electronic

notarization parallels the customary legal form of notarization. The notary public shall require that the signatories provide such authentication information as required by law, typically a government issued photo identification card and a biometric submission, such as a signature or a thumbprint. VVSC employee notary public will have the means to verify hard copy personal identification, such as a drivers license information and to input said information electronically in the form of a source code. Likewise, VVSC employee notary public will have the means to verify the electronic signature of the party and to input said information electronically in the form of a source code. Per the methodology above, the input information is displayed on the browser of the local computer system as a separate dual image.

[0105] Upon input of the personal verification information, VVSC notary public affixes an electronic notary seal to the electronic document. Per the preferred embodiment of the present invention, the electronic notary seal is in the form of a graphical representation of the notary public's seal. The graphical representation is affixed to the electronic document as a visual image. Alternatively, the notary seal may be affixed to the document in the form of a source code. Any changes to the electronic document will invalidate the notary public's seal.

///

[0164] 4. Electronic Notary Device

[0165] An electronic notary device will be necessary for the method of the present invention. The function of the electronic notary device will be to provide electronic notarization to electronic documents. The electronic notary stamp is affixed to the electronic document in one of two ways: by manually imprinting the notary seal using the electronic signature capture device pad and the conventional notary stamp, or, alternatively, by utilizing an electronic device that is encrypted with the equivalent of the notary's stamp in the form of source code which is affixed to the electronic document. The present invention will electronically affix the electronic notary seal to verify either a signature that is in a graphical format (using an electronic signature capture device) or an electronic format (using a digital certificate).

[0180] Notary public: The term "notary public" or "notarization" shall be construed to mean authenticating a document using, but not limited to, the following means: a live commissioned notary public; another person certified to authenticate documents; digital forms of notarizing documents such as a digital certificate and the technology identified in United States pending patent application, herein identified as Customer 021907.



#### PARAGRAPH 19

Paragraph 19 (as amended herein) reads: Another problem with conventional real-time videoconferencing methods is that none of the existing systems or applications incorporate a system, method or process whereby a client may tender a service request for videoconference authentication from a remote location using the Internet.

Examiner submits that the original disclosure does not disclose a service request using the internet. Applicant respectfully traverses. Support for paragraph 19 from the original disclosure is as follows:

#### CLAIMS IN SUPPORT OF PARAGRAPH 19

Applicant respectfully refers Examiner to claims 1, 24, 51, 52, and 53 of the original disclosure. In particular claims 51-53 specifically and particularly discloses the internet (world-wide-web) as a means to use the inventive device.

1. A method and system for performing identity and signature and document authentication using a videoconference; said method and system comprising: a host computer server, a multi-point and multi-media video conference system (including fixed and portable structures), an electronic signature capture device, an electronic document, an electronic document repository, a digital certificate, an electronic notary seal device,

a biometric data capture device, and a video verification service center (VVSC); said method and system comprising the steps of: said VVSC establishing connectivity between geographically remote parties; said connectivity comprising a videoconference that broadcasts electronic data between said parties using said multi-point and multi-media video conference system; said parties viewing one another from said multi-point and multi-media video conference system; said VVSC downloading said electronic document from said host computer server; said parties viewing the same said electronic document from said multi-point and multi-media video conference system; said parties inputting an electronic signature using said electronic signature capture device; said host computer server affixing said electronic signature to said electronic document; said parties inputting biometric data using said electronic biometric data capture device; said host computer server affixing said biometric data to said electronic document; said parties inputting said digital certificate; said host computer server affixing said digital certificate to said electronic document; said electronic notary seal device inputting an electronic notary seal; said host computer server affixing said electronic notary seal to said electronic document; said host computer server encrypting said electronic document; said host computer server uploading said electronic document to said host computer server; and said VVSC disseminating said electronic document to said parties.

24. A method and system for performing identity and signature and document authentication using a videoconference; said method and system comprising: a host computer server, a multi-point and multi-media video conference system (including fixed and portable structures), an electronic signature capture device, an electronic document, an electronic document repository, a digital certificate, an electronic notary seal device, a biometric data capture device, and a video verification service center (VVSC); said method and system comprising the steps of: said VVSC establishing connectivity between geographically remote parties; said connectivity comprising a videoconference that broadcasts electronic data between said parties using said multi-point and multi-media video conference system; said parties viewing one another from said multi-point and multi-media video conference system; said VVSC downloading said electronic document from said host computer server; said parties viewing the same said electronic document from said multi-point and multi-media video conference system; said parties inputting an electronic signature using said electronic signature capture device; said host computer server affixing said electronic signature to said electronic document; said parties inputting biometric data using said electronic biometric data capture device; said host computer server affixing said biometric data to said electronic document; said parties inputting said digital certificate; said host computer server affixing said digital certificate to said electronic document; said host computer server encrypting said electronic document; said host

computer server uploading said electronic document to said host computer server or to a remote server of said parties; said host computer server creating an identity-based document with said electronic document; and said host computer server disseminating said identity-based document to authorized said parties.

51. A method and system for performing identity and signature and document authentication using a videoconference conducted via the World-Wide-Web (WWW); said method and system comprising: a host computer server, a local computer system, a multi-point and multi-media video conference system (including fixed and portable structures), a website, an electronic signature capture device, an electronic document, an electronic document repository, a digital certificate, an electronic notary seal device, a biometric data capture device, and a video verification service center (VVSC); said method and system comprising the steps of: said local computer system using Internet connectivity to access said website; said local computer system establishing connectivity between geographically remote parties via said website; said connectivity comprising a videoconference that broadcasts electronic data between said parties using said multi-point and multi-media video conference system and said website; said parties viewing one another from said multi-point and multi-media video conference system; said local computer system downloading said electronic document from said host computer

server; said parties viewing the same said electronic document from said multi-point and multi-media video conference system; said parties inputting an electronic signature using said electronic signature capture device; said host computer server affixing said electronic signature to said electronic document; said parties inputting biometric data using said electronic biometric data capture device; said host computer server affixing said biometric data to said electronic document; said parties inputting said digital certificate; said host computer server affixing said digital certificate to said electronic document; said electronic notary seal device inputting an electronic notary seal; said host computer server affixing said electronic notary seal to said electronic document; said host computer server encrypting said electronic document; said host computer server uploading said electronic document to said host computer server; and said host computer server disseminating said electronic document to said parties.

52. The method of claim 51 whereby said host computer server further comprises the means to operate said website; said website allows said parties to access and use the inventive device and to manage the transactions contemplated therein.

53. The method of claim 51 whereby said parties may be a plurality of

parties, each with the ability to participate simultaneously in said videoconference using said local computer system.

#### DISCLOSURE IN SUPPORT OF PARAGRAPH 19

Applicant respectfully further refers Examiner to paragraphs 16, 17, 18, 19, 29, 68, 69, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, and 106 of the original disclosure.

[0016] The main problem with conventional real time video conferencing methods is that none of the existing systems or applications incorporate a system, method or process of electronic identity authentication of the geographically remote individuals to the videoconference.

[0017] Another main problem with conventional real time video conferencing methods is that none of the existing systems or applications incorporate a system, method or process of electronic signature authentication of the geographically remote individuals to the videoconference.

[0018] Another problem with conventional real time video conferencing methods is that none of the existing systems or applications incorporate a system, method or process of electronic document authentication as part of the transaction by the geographically remote individuals to the

videoconference.

[0019] Another problem with conventional real time video conferencing methods is that none of the existing systems or applications incorporate a system, method or process of electronic authentication of one's identity, signature and the documents simultaneously of the geographically remote individuals to the videoconference.

[0029] The WWW embodiment is put into context by way of the following example. Assume that a customer requires an authenticated student identification card. The customer need not travel to the university for the creation of such a card but may input the required information from the convenience of home. The customer accesses the present invention on the WWW using a configured graphic user interface (GUI). Utilizing the GUI, the customer may input electronic data using a home personal computer. The customer will be prompted to input varied forms of electronic data, including, but not limited to, an electronic signature, including a graphical hand written signature, a photographic image, biometric data, such as a thumbprint, or electronic data in the form of a code or a password. The electronic data input is verified by the present inventive method and amalgamated into an authenticated student card which is issued to the authorized party, presumably the student in this instance.

[0068] The present invention is premised on the concept of an increasingly borderless world, insofar as technology and the Internet have ever more united remote parties in a host of transactions that once would have necessitated an actual, physical face-to-face meeting. By way of example, one may execute electronic documents online on the Internet using forms of electronic signatures, thereby eliminating the need for the signatories to coordinate a face-to-face meeting. Likewise, one may scan personal biometric data, such as a thumbprint, and submit such data via an electronic upload to a remote database, thereby eliminating the need to manually fingerprint oneself and mail such hard copy information. Remarkably, with ease we now videoconference using desktop computers and telephonic devices that allow geographically remote parties to simultaneously view and hear one another via the Internet.

[0069] All of these technologies function to eliminate the need to arrange an actual physical meeting to facilitate a host of transactions. The present invention seeks to coordinate such borderless processes for a method and system of remote party collaboration not rendered by the prior art using a real time, live stream videoconference to enjoin the parties. In the preferred embodiment of the present invention, a customer accesses a remote facility to process a verification request of the customer's identity or the customer's signature, with the purpose of the verification to create



an authenticated electronic document.

[0095] III. Identity, Signature, and Document Authentication Using a Local Computer System and the World-Wide-Web

[0096] In yet another embodiment of the present invention, the parties to the transaction utilize the inventive device independent of the VVSC and independent of a traveling VVSC representative. In this embodiment of the present invention, the parties to the transaction initiate a videoconference via a website that is a function of the VVSC. The web-based VVSC application has a two-fold function: it allows parties to conduct private transactions using a videoconference broadcast via the WWW (webconference), secondly, and it allows registered users to submit electronic data to the VVSC for retrieval and/or dissemination to other parties.

[0097] As a priori, to use the present invention from a location independent from a VVSC and independent of a traveling VVSC representative., i.e. the WWW, the customer first must register with the VVSC at its physical location. Registration comprises the VVSC obtaining and verifying personal information from the customer using a variety of data, such as electronic data, government issued personal identity documents, biometric data, such as an electronic signature, a thumbprint

and the like, a digital certificate or other such data as may be available.

Upon registration, VVSC issues the customer personal identification documents from VVSC, including, but not limited to, a digital certificate, a smart card, a password or a code. VVSC may keep a record of customer's biometric information for future use, should customer elect to do so.

[0098] To initiate a transaction independent of the VVSC, a customer wishing signature or identity verification or electronic document creation utilizes the present invention via a local computer system to interface with the VVSC website located on the World Wide Web (WWW). The customer accesses the website via the local computer system and logs in using the password or code as provided by VVSC in the registration process. As per the methodology depicted above, a videoconference is initiated by the VVSC between the parties using a real time, live stream webconference. All parties to the transaction must be registered with the VVSC.

[0099] An authentication transaction request using the VVSC website necessitates that the customer use a VVSC graphic user interface (GUI) which runs from the local computer system. The GUI comprises the means for the browser of customer local computer system to display multiple images simultaneously on the monitor of said customer local computer system per the methodology of the preferred embodiment. Said multiple images further comprise: the remote parties to the transaction, the

electronic data that is to be input by the parties, and the electronic document that is to be created or authenticated. Not every transaction will comprise every image, the images displayed are dependent on the transaction request.

[0100] The webconference method of the inventive device will be most useful in facilitating private e-commerce transactions wherein the parties to the transaction need to ascertain the identity and actual signature of the parties to the transaction. In this aspect, geographically remote individuals may conduct high value or sensitive transactions that necessitate authentication of one's signature to the agreement using the inventive device to webconference with one another, and using the inventive device to exchange electronic data, such as an electronic signature, a photograph, a fingerprint, or an electronic file during the webconference.

[0101] Upon initiation of a webconference, the parties to the transaction may opt to upload an electronic document from the local computer system to the VVSC host computer server for electronic data input. Alternatively, the parties may elect to download an electronic document from the electronic document repository maintained by the present invention. The electronic document repository comprises a library of electronic documents designed to facilitate e-commerce, including, but not limited to, deeds of trust, mortgages, promissory notes, affidavits, assignments and

so on. Upon either uploading a document, or selecting a document for download, VVSC will structure the transaction request and manage the transaction cycle.

[0102] Per the methodology of the preferred embodiment, the electronic document to be executed is depicted along with an electronic image of the electronic signature being affixed to the document as a graphical, hand written representation or as form of source code, and the actual party executing the electronic signature. Said images are displayed on the browser of the local computer system in the manner of a screen or monitor hosted at an independent VVSC.

[0103] Upon affixation of each electronic signature to the electronic document, the browser of the local computer system depicts the signed electronic document. In the preferred embodiment, the electronic data may be affixed to the electronic document as a visual representation of a graphical hand-written signature. Alternatively, the electronic data may be affixed to the electronic document in the form of encrypted source code. Should other electronic data be required, such as a photographic image, a thumbprint, or a code, it will be entered in subsequent fashion and displayed on the browser of the local computer system. By way of example, in addition to affixing an electronic signature to the electronic document, the parties may request further authentication information such

as a drivers license number, a thumbprint, or a photographic image. As such other authentication data is entered, the respective information is displayed on the browser of the local computer system as a separate image, and is affixed to the electronic document where indicated. In the preferred embodiment, the electronic data may be affixed to the electronic document as a graphic, visual representation. Alternatively, the electronic data may be affixed to the electronic document in the form of encrypted source code.

[0104] Per the method of the preferred embodiment, the webconference is capable of providing electronic notarization services to the parties. The notary public may be an employee who is physically located at the VVSC or may be a remote party enjoined by the webconference. Electronic notarization parallels the customary legal form of notarization. The notary public shall require that the signatories provide such authentication information as required by law, typically a government issued photo identification card and a biometric submission, such as a signature or a thumbprint. VVSC employee notary public will have the means to verify hard copy personal identification, such as a drivers license information and to input said information electronically in the form of a source code. Likewise, VVSC employee notary public will have the means to verify the electronic signature of the party and to input said information electronically in the form of a source code. Per the methodology above, the input

information is displayed on the browser of the local computer system as a separate dual image.

[0105] Upon input of the personal verification information, VVSC notary public affixes an electronic notary seal to the electronic document. Per the preferred embodiment of the present invention, the electronic notary seal is in the form of a graphical representation of the notary public's seal. The graphical representation is affixed to the electronic document as a visual image. Alternatively, the notary seal may be affixed to the document in the form of a source code. Any changes to the electronic document will invalidate the notary public's seal.

[0106] Upon affixing the required authentication information, including, but not limited to, an electronic signature, a photographic image, biometric information, source code, an electronic notary seal, the customer uploads the electronic document to the VVSC web server from the local computer system. The VVSC fuses the respective electronic data input from the remote parties into a single, authenticated electronic document. The single authenticated document is then assigned a time and date stamp and a password. No changes may be made to the electronic document without detection. The password is disseminated to those parties authorized to retrieve a copy of the authenticated document from the VVSC web server. Logging into the server via the local computer system, authorized parties

Application Number 09/973, 273

download the single, authenticated electronic document using the password provided from the WVSC.

#### PARAGRAPH 20

Paragraph 20 (as amended herein) reads: Another problem with conventional real-time videoconferencing methods is that none of the existing systems or applications incorporate a system, method or process whereby an authoritative document is created and issued during the videoconference.

Examiner submits that the original disclosure does not disclose the issuance of a final or authoritative document. Applicant respectfully traverses. Support for paragraph 20 from the original disclosure follows.

#### CLAIMS IN SUPPORT OF PARAGRAPH 20

Applicant respectfully refers Examiner to claims 1,6, 7, 22, 24, 33, 47, 50, 75, 76, and 77 of the original disclosure.

1. A method and system for performing identity and signature and document authentication using a videoconference; said method and system comprising: a host computer server, a multi-point and multi-media video conference system (including fixed and portable structures), an electronic signature capture device, an electronic document, an electronic document repository, a digital certificate, an electronic notary seal device,

a biometric data capture device, and a video verification service center (VVSC); said method and system comprising the steps of: said VVSC establishing connectivity between geographically remote parties; said connectivity comprising a videoconference that broadcasts electronic data between said parties using said multi-point and multi-media video conference system; said parties viewing one another from said multi-point and multi-media video conference system; said VVSC downloading said electronic document from said host computer server; said parties viewing the same said electronic document from said multi-point and multi-media video conference system; said parties inputting an electronic signature using said electronic signature capture device; said host computer server affixing said electronic signature to said electronic document; said parties inputting biometric data using said electronic biometric data capture device; said host computer server affixing said biometric data to said electronic document; said parties inputting said digital certificate; said host computer server affixing said digital certificate to said electronic document; said electronic notary seal device inputting an electronic notary seal; said host computer server affixing said electronic notary seal to said electronic document; said host computer server encrypting said electronic document; said host computer server uploading said electronic document to said host computer server; and said VVSC disseminating said electronic document to said parties.



6. The method of claim 1 whereby said electronic document further comprises digital or electronic documents in various mediums, whether tangible or not (i.e. source code, compact disc, floppy diskette).

7. The method of claim 1 whereby said electronic document may be applicable to an array of transactions, such as banking, real estate, identity based documents and law.

22. The method of claim 1 whereby said host computer server further comprises the means to encrypt said electronic document.

24. A method and system for performing identity and signature and document authentication using a videoconference; said method and system comprising: a host computer server, a multi-point and multi-media video conference system (including fixed and portable structures), an electronic signature capture device, an electronic document, an electronic document repository, a digital certificate, an electronic notary seal device, a biometric data capture device, and a video verification service center (VVSC); said method and system comprising the steps of: said VVSC establishing connectivity between geographically remote parties; said connectivity comprising a videoconference that broadcasts electronic data between said parties using said multi-point and multi-media video conference system; said parties viewing one another from said multi-point

and multi-media video conference system; said VVSC downloading said electronic document from said host computer server; said parties viewing the same said electronic document from said multi-point and multi-media video conference system; said parties inputting an electronic signature using said electronic signature capture device; said host computer server affixing said electronic signature to said electronic document; said parties inputting biometric data using said electronic biometric data capture device; said host computer server affixing said biometric data to said electronic document; said parties inputting said digital certificate; said host computer server affixing said digital certificate to said electronic document; said host computer server encrypting said electronic document; said host computer server uploading said electronic document to said host computer server or to a remote server of said parties; said host computer server creating an identity-based document with said electronic document; and said host computer server disseminating said identity-based document to authorized said parties.

33. The method of claim 24 whereby said host computer server further comprises the means to download said electronic document from said repository and to display said electronic document on said screen or monitor of said multi-point and multi-media video conference system.

47. The method of claim 24 whereby said host computer server further

comprises the means to create said identity-based document from said electronic document.

50. The method of claim 24 whereby said host computer server disseminates said identity-based document to authorized said parties.

75. The method of claim 51 whereby said host computer server further comprises the means to create said identity-based document from said electronic document.

76. The system of claim 75 whereby said identity-based document further comprises a variety of forms, whereby said identity-based document comprises a tangible hard copy document, or whereby said identity-based document comprises intangible source code, or whereby said identity-based card comprises a combination of both.

77. The system of claim 76 whereby said identity-based document further comprises a variety of said electronic data, including, but not limited to said biometric data.

DISCLOSURE IN SUPPORT OF PARAGRAPH 20

Applicant respectfully further refers Examiner to paragraphs 15, 18, 23, 24, 25, 26, 27, 47, 56, 57, 64, 66, 69, 87, 88, 89, 90, 92, 92, 94, and 181 of the original disclosure.

[0015] The prior art fails to disclose any videoconference method whereby signature authentication or identity authentication may be conducted during the videoconference. The prior art fails to disclose any videoconference method whereby electronic data may be captured and input during the video conference. The prior art fails to disclose an videoconference method whereby the respective electronic data input from any party is verified, and fused in a single, authenticated electronic document.

[0018] Another problem with conventional real time video conferencing methods is that none of the existing systems or applications incorporate a system, method or process of electronic document authentication as part of the transaction by the geographically remote individuals to the videoconference.

[0023] The general purpose of the present invention, which will be described subsequently in greater detail, is to provide a new method of real time video conference for electronic identity and signature

authentication, and for electronic document creation and authentication, that has the many advantages mentioned heretofore and many novel features that result in a new videoconference method which is not anticipated, rendered obvious, suggested, or even implied by any of the prior art video conferencing, either alone or in any combination thereof.

[0024] The present invention incorporates a variety of applications and technology that in conjunction can be used to authenticate a personal identity, a signature, or an electronic document, either singularly or simultaneously, during a real time, live stream videoconference. The nature of the transaction is dependent on the needs of the parties to the videoconference. For example, the parties may need identity authentication, or signature authentication, or electronic document creation and authentication, or a combination of all three.

[0025] Likewise, the form and type of authentication will vary depending on the needs or requests of the parties. The present invention is capable of a broad base of applications that result in authentication. The method of the present invention utilizes signature data, biometric data, photographs, electronic data input and electronic notarization. Any particular form of authentication may be used singularly or in conjunction with another form of authentication. The purpose of the electronic data capture is to create an authenticated document, such as an executed contract, a passport or

drivers license, and the like. The present invention is capable of authenticating any type of document and the foregoing examples are not regarded as limiting. Likewise, it should be understood that the foregoing examples of authentication are all conducted between geographically remote parties during a real time, live stream videoconference.

[0026] By way of example, a standard real estate transaction is detailed. Such a transaction typically requires that geographically remote parties physically meet to confirm the identity of one another or that they travel to a notary public to have their identities authenticated. Such a process is time consuming, expensive and inconvenient. Using the present invention, a transfer of title to property would unite the buyer in New Jersey, the seller in California, and the e the notary public in New York in a three way real time, live stream video conference. The geographically remote parties are each able to view one another via a video and audio stream. The parties may each input electronic data, in this instance, a signature, into a single electronic document using the means of the present invention. Upon input of the respective electronic data from the dispersed parties, the present invention serves to manage the electronic data input and generate the desired electronic document. By way of the foregoing example, the result would be a single, authenticated electronic document that is executed by the dispersed parties. A time and date stamp is affixed to the electronic document so that no changes may be made to the

encrypted document. The single, finalized notarized electronic document is then issued to the authorized receiving party, such as the registrars office.

[0027] In another embodiment, the present inventive method enjoins a customer with a remote governmental agency in a real time, live stream videoconference. In this embodiment, the present invention inputs electronic data from the customer for the purpose of creating an authenticated government issued document, such as a drivers license or a passport. Per the foregoing example, the electronic data input may comprise various forms, including, but not limited to, an electronic signature, a photographic image, biometric data, such as a thumbprint, or electronic data in the form of a code or a password. Using the inventive device, said governmental agency in turn verifies the electronic data input as being authentic. Upon authentication of the input information, an electronic document is created that encapsulates the input electronic data with the document requested, such as a passport or social security card.

[0047] (xvi) the means to authenticate an electronic document that has electronic data fused to it; and

[0056] Another object of the present invention is to provide a method of identity, signature, and electronic document authentication using a real

time, live stream videoconference platform that fuses the electronic data input by the parties to the electronic documents created through the method of the present invention.

[0057] Another object of the present invention is to provide a method of identity, signature, and electronic document authentication using a real time, live stream videoconference platform that allows an individual, via an interface with the present invention, direct communication with government and other regulatory agencies to create hard copy identity-based cards or documents that are encoded with various electronic and biometric information.

[0064] FIG. 3 The present invention processes' are somewhat codependent insofar that the process of either identity and signature verification inherently result in an authenticated document. FIG. 3 depicts the steps and/or methods utilized to create, secure and store an electronic document.

[0066] The present invention recognizes that there is much more to live stream videoconference collaboration than just the video and audio experience. The present invention offers solutions that blend video and audio communication with various forms of electronic data input with a real time, live stream videoconference. Specifically, the present invention is a



process, method and system that uses a videoconference system to input and transmit electronic data for the purpose of authenticating an identity, a signature or to create an authenticated electronic document using a real-time, live-stream videoconference medium.

[0069] All of these technologies function to eliminate the need to arrange an actual physical meeting to facilitate a host of transactions. The present invention seeks to coordinate such borderless processes for a method and system of remote party collaboration not rendered by the prior art using a real time, live stream videoconference to enjoin the parties. In the preferred embodiment of the present invention, a customer accesses a remote facility to process a verification request of the customer's identity or the customer's signature, with the purpose of the verification to create an authenticated electronic document.

#### [0087] II. Identity Card Creation Authentication Using a VVSC

[0088] In another embodiment of the present invention, the inventive device functions to create personal-identity cards for regulatory agencies, educational institutions, or the private sector. This embodiment functions per the methodology of the first embodiment but with a different objective. As opposed to facilitating e-commerce transactions, the inventive device is used to verify identity and issue authoritative documents. By way of

example, a government agency may require authoritative authentication to issue a state sponsored identification card, such as a passport, a social security number or a drivers license.

[0089] The customer requiring an identity-based document goes to an independent VVSC that is conveniently located in proximity with their physical location. The VVSC initiates a videoconference with all of the parties to the transaction: the customer and the respective government agency. Per the preferred embodiment, the videoconference comprises screens or monitors at each location whereby the parties can input and receive audio, visual and electronic data simultaneously, albeit independently at each location.

[0090] Upon initiation of the videoconference, VVSC downloads the specific electronic document from the electronic document to a central host computer that is to become a particular identity-based document. The downloaded electronic document is displayed on a screen or monitor for the respective parties to see, each party viewing the same electronic document. Likewise, the screen or monitor comprises split images that are viewed simultaneously: one of the remote party, one of the identity-based electronic document to be created, one of the electronic data being input and other such multiple imaging as necessary.

[0092] Per the method of the preferred embodiment, the present invention comprises the means whereby as the customer electronically signs the electronic document, the electronic data being input is displayed on the screen or the monitor of the requesting agency. The requesting agency to the videoconference is thereby viewing a single screen with dual images: the customer, the identity-based electronic document, and the electronic signature as it is being captured. Upon affixation of each electronic signature to the identity-based electronic document, the screen or monitor will depict the signed identity-based electronic document. In the preferred embodiment, the electronic data may be affixed to the electronic document as a visual representation. Alternatively, the electronic data may be affixed to the electronic document in the form of encrypted source code.

[0093] Should other electronic data be required, such as a photographic image, a thumbprint, or a code, it will be entered in subsequent fashion and displayed on the screen or monitor. By way of example, in addition to affixing an electronic signature to the electronic document, the requesting agency may request further authentication information such as a driver's license number, or a thumbprint. As such other authentication data is entered, the respective information is displayed on the screen or monitor as a separate image, and is affixed to the electronic document where indicated. In the preferred embodiment, the electronic data may be affixed

to the electronic document as a visual representation. Alternatively, the electronic data may be affixed to the electronic document in the form of encrypted source code.

[0094] As the foregoing example clearly illustrates, the present invention has the potential to facilitate transactions where the parties are in different cities, states or even countries. An American traveler who loses a passport in India may find A VVSC, videoconference with the issuing authority, and have a new passport electronically created and issued without the wait, expense or inconvenience of traditional channels.

[0181] Electronic Document: The term "electronic document" shall be construed to mean any data that is constructed and compiled by use of the present invention; including but not limited to, digital or electronic documents in various mediums, whether tangible or not (i.e. source code, compact disc, floppy diskette, etc.); documents encompassing an array of transactions and documents comprised of tracking, managing and storing information created by use of the invention.

## **DRAWINGS**

Per page 4, paragraph 4, of the final office action, Examiner objects to the drawings because they contain new matter. Applicant respectfully traverses.

Application Number 09/973, 273

Applicant submits that the original drawings failed to fully depict the claimed invention, as disclosed in the original specification, and that the replacement drawings fully depict the claimed invention in the original specification.

With respect to FIG 1 (Identity Authentication Services/Overview), Applicant refers to the original specification in its entirety.

With respect to FIG 1A (Identification Criteria), Applicant refers to paragraph 76 through 79, and paragraph 91, and paragraph 93 of the original specification.

With respect to FIG 2 (Authentication Using a Notary), Applicant refers to paragraph 72 through 84 and paragraphs 88 through 93, of the original specification.

With respect to FIG 2A (Authentication Using a Notary at VVSC whereby VVSC downloads document), Applicant refers to paragraph 72 through 84 and paragraphs 88 through 93, of the original specification.

With respect to FIG 2B (Signature Authentication Using a Notary at VVSC whereby VVSC uploads document), Applicant refers to paragraph 72 through 84 and paragraphs 88 through 93, of the original specification.

With respect to FIG 3-3A (Authentication Using VVSC Website), Applicant refers to paragraph 72 through 84 and paragraphs 88 through 93, and paragraphs 96-106 of the original specification.

Application Number 09/973, 273

With respect to FIG 3B-3D (Authentication Using VVSC Website Whereby a Notary is Required), Applicant refers to paragraph 72 through 84 and paragraphs 88 through 93, and paragraphs 96-106 of the original specification.

With respect to FIG 3D (Identification Criteria), Applicant refers to paragraph 76 through 79, and paragraph 91, and paragraph 93 of the original specification.

With respect to FIG 3E (Client Registration), Applicant refers to paragraph 96 through 98 of the original specification.

## **DEFINITIONS**

Per page 4, paragraph 5, of the final office action, Examiner objects to the paragraphs as containing new matter. Applicant requests that paragraphs 178-184 of the substitute specification be deleted in their entirety and replaced with the following text:

Video Authentication Service Center (VVSC)

The VVSC is a physical structure, a place of business, where either a client or a customer can go to process a service request, The VVSC is staffed by VVSC employees and is equipped with the infrastructure to enable the service requests, as disclosed herein. The VVSC enables the service request tendered by the client and coordinates the schedule of the parties to the videoconference.

The VVSC establishes the time and date and locations for the real-time videoconference between the client and customer(s). All parties to the videoconference receive a confirmation prior to the videoconference via electronic mail or other forms of messaging, such as text, or mail or telephone, informing said parties of the time, date and location of the videoconference. The parties are advised of the contents of the service request, and the necessary identity criteria that must be provided during the videoconference. The VVSC enables and manages the services requested by the client; irrespective of the different location of the client and customer. The VVSC provides the necessary infrastructure and applications for the videoconference, the service request, and to create the finalized authoritative document.

#### Video Authentication Service Center Website (VVSC website)

In the preferred embodiment, the VVSC website is accessible via the Internet. The VVSC website provides the service requests disclosed herein: identity, or signature, or document authentication. The VVSC website enables a client or a customer to access authentication services from a local computer system (e.g. their home or office), without having to physically visit a VVSC.

The VVSC website establishes the time and date and locations for the real-time videoconference between the client and customer(s). All parties to the videoconference receive a confirmation prior to the videoconference via electronic mail or other forms of messaging, such as text, or mail or telephone, informing said parties of the time, date and location of the videoconference. The parties are advised of the contents of the service request, and the necessary identity criteria that must be provided during the website videoconference. The VVSC enables and manages the services requested by the client; irrespective of the different location of the client and customer. The VVSC provides the necessary infrastructure and applications for the website videoconference, the service request, and to create the finalized authoritative document.

#### Service Request or Request for Services

A service request, or request for services; used interchangeably, mean a request from a client for any of the foregoing services from the VVSC or the VVSC website. Specifically: identity authentication, or signature authentication, or document authentication, or any combination thereof. Irrespective of the client's service request, it is processed in the context of a real-time videoconference. A client may tender a single service request, or multiple service requests, to be fulfilled in the course of the videoconference.



#### Client and Customer

A client is the individual tendering the service request to the VVSC or the VVSC website. A customer is the individual whose identity, or signature, or documents are being authenticated. In some transactions, a client may also request that the client's identity, or client's signature, or client's document be authenticated during the videoconference, along with the customer's. By way of example, a client and a customer may wish to verify the identity and signature of one another to conclude a commercial transaction, such as the purchase of real estate, during the videoconference. In this instance, each party would input identifying criteria to be authenticated by the VVSC. It is to be understood that there may be multiple clients, or customers involved in a single videoconference. Collectively, the group of individuals participating in the videoconference are referred to as "the Parties".

#### Governmental Agency (Public) and Private Party (Private)

A distinction is made between the type of client tendering a service request. A public client is deemed to be a governmental agency (G.A.) such as the D.M.V. or the USPS, and a private party is deemed to be an individual or business from the private sector.

#### Identifying Criteria or I.D. Criteria

Identifying criteria, or I.D. criteria; used interchangeably, comprise the data input that was used to authenticate either an identity, a signature, or a document. Likewise, identifying criteria is used to create the authoritative document. The identifying criteria for an individual is at least one of a group of: a signature, a fingerprint, a retina scan, a voiceprint, a hard copy identity document, a photograph, or a password/ code. Depending on the service request, a client may select any combination of the I.D. criteria to authenticate the customer, and any combination of the I.D. criteria to create the authoritative document. The identifying criteria of a public entity include at least one of a group of a hard-copy identity document, a password/ code, a signature, proof of executive identity/authority, a corporation number, or a photograph.

#### Authentication

Authentication (and variations on the verb thereof), are used interchangeably, and mean the process whereby either an identity, or a signature, or a document is authenticated in accordance with the client's service request.

#### Authoritative Document (A.D.)

The authoritative document contains the identity criteria information requested by the client in the service request.

Depending on the service request, the resulting authoritative document is comprised of at least one of the following group: a signature, a fingerprint, a retina scan, a voiceprint, a hard copy identity document, a photograph, or a password/ code. The authoritative document is created during the real-time videoconference. The authoritative document is issued during the real-time videoconference. In the preferred embodiment, the authoritative document is issued in the form of an identity card such as a passport or drivers license. The authoritative document can also be issued as an electronic document or electronic code that is stored in a hardware device, such as a disc or chip. Regardless of the form of the authoritative document, each authoritative document is encrypted with the I.D. criteria input and secured with a time and date stamp.

#### Videoconference or Webconference

The term videoconference or webconference means a real-time video-communication between the parties . The present invention may use various videoconference technologies and applications thereof, but all are premised on the fact that it is a real time transaction between the parties that are remote in location. The videoconference enables the exchange of visual and audio

communication between the parties, in addition to enabling the transaction of the service request.

#### Document

An electronic document is used in the method of the present invention. The function of the electronic document repository is to fulfill the client service request. The electronic document may comprise audio, video, graphic, biometric, or text data. A client may elect to download an electronic document from an electronic document repository maintained by the present invention.

Alternatively, a client may elect to upload an electronic document to enable the client service request. The VVSC electronic document repository contains a library of electronic documents typically used in public and private party transactions: Oaths, promissory notes, deeds, etc.. It is to be understood, that reference to a document means an electronic document, except where qualified as a hard copy document.

#### Electronic Signature Capture Device

An electronic signature capture device is used in the method of the present invention. The electronic signature capture device captures the electronic signatures of the parties to the transaction. The electronic signature capture device is capable of assigning digital

code, or a graphic image, or both to the authoritative document.

The graphical representation depicts the actual hand-written signature of the signatory.

### Signature

The term signature shall be construed to mean any form of electronic signature, including at least one of the group of a graphical, hand written representation, a digital certificate, a password, or other electronic data input qualified to constitute a signature.

### Notary Public and Notarization

The term notary public and notarization means the process of authenticating a electronic document by a live, human-being commissioned notary public. The notary public notarizes the document in accordance with the law.

### Electronic Notary Device

An electronic notary device is used for the method of the present invention. The electronic notary device provides a method of electronic notarization to verify a signature or an individual or the contents of a document. An electronic notary stamp is affixed to a

Application Number 09/973, 273

document in one of two ways: by manually imprinting the notary seal using the electronic signature capture device pad, or, alternatively, by utilizing an electronic device that is encrypted with the equivalent of the notary's stamp in the form of source code which embeds the notary code in the authoritative document.

## **CLAIMS**

Applicant presents the claims with the current status of each claim (as amended in Applicant's response to the First Office Action) identified.

Claims 1-4, 8-28, 30-56, 59-74 are pending.

Claims 6, 7, 29, 57, 58, 75, 76, and 77 are canceled.

Claim 78 is new.

## **APPLICANT RESPONSE TO THE OFFICE ACTION**

Having amended the substitute specification in accordance objections raised in the Final Office Action, Applicant responds to the substantive arguments presented by Examiner, as put forth below.

### **CLAIM REJECTIONS UNDER 35 U.S.C. § 112**

Applicant notes Examiner's objections to claims 1-5, 8-28i, 30-56, 59-74 and 78 with respect to 35 U.S.C. § 112. Applicant respectfully traverses. Applicant respectfully submits that the amended claims (appended hereto) address the foregoing noted informalities raised pursuant to U.S.C. § 112. Applicant further submits the claims, as amended, are in condition for allowance, and respectfully requests that the Examiner's objections be withdrawn.

### **CLAIM REJECTIONS UNDER 35 U.S.C. § 103**

#### **OBVIOUSNESS**

Examiner has rejected claims 1-77 of the pending application as being unpatentable over US Application 2001/0002485 (hereinafter referred to as "Bisbee")<sup>2</sup> in view of US Patent 5,712,914 (hereinafter referred to as "Aucsmith") further in view of US Patent No. 6, 317,777 (hereinafter referred to as "Skarbo").

---

<sup>2</sup> Applicant respectfully submits that the Examiner's arguments may have been rendered moot with respect to the Bisbee application; said application was issued a final rejection by the USPTO on 3/21/2005 and again on 01/05/2006. Applicant notes that a RCE was filed with the USPTO on 7/13/2005, and on 03/06/2006, respectively.

Application Number 09/973, 273

Applicant respectfully submits that Examiner's position is traversed. Applicant respectfully requests that the Examiner reconsider the 35 U.S.C. §103 objection in accordance with the arguments put forth below.

Applicant wishes to address the substantive arguments put forth by the Examiner under 35 U.S.C. § 103 on the basis of obviousness; addressing the Examiner's objections in turn as put forth in the office response.

### **U.S.C. § 103 ANALYSIS**

Examiner submits that claims 1-77 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bisbee (US Patent Application Publication 2001/0002485), in view of Aucsmith in further view of Skarbo et al.

With reference to paragraph 12, lines 4-13, pages 6-7, Examiner cites the prior art of Bisbee as disclosing

“...a system wherein a set of parties in a networked architecture, using Transfer Agents, use a server, a Document Authentication System (DAS), in conjunction

with a notary, called a TCU. Electronic documents are transmitted to the TCU via a communication means.... The Transfer Agent relays to the TCU a set of authentication data, including digitized hand-written signatures, biometric



information, and a digital signature (certificate), which have been acquired by a transfer agent from the appropriate means.

Upon authentication of the information provided by the transfer agent, the TCU appends a certificate to the document to confirm authenticity, but does not append the biometric data, or certificates supplied by the transfer agents."

[Emphasis mine].

Applicant notes paragraphs 69-70 of Bisbee which read:

[0069] The information object is digitally signed and/or encrypted and the authentication certificate is appended by the DAS, thereby attesting to the fact that the Transfer Agent witnessed the participants sign the electronic document. The digitally signed and/or encrypted document may be electronically communicated to the TCU via a modem or computer network block 112). Other ways of communicating digitally signed or encrypted documents might be used (for example, dispatching a diskette containing the document), but the great advantage of

electronic communication is speed. [Emphasis mine]

[0070] In addition, although it is currently believed to be preferable for the Transfer Agent to digitally sign an information object before submitting the result to a TCU, it is only necessary for the Transfer Agent to "sign" an information object in a way that can be understood, legally or otherwise, as the Transfer Agent's attesting to the integrity and validity of the information object. For example, the Transfer Agent might append to an information object a digitized hand-written signature, a digitized signature and verifiable biometric information, a digital signature, or a combination of these. Alternatively, the Transfer Agent can sign an information object by connecting to a TCU using the password and other procedures of a secure protocol, such as the secure sockets layer (SSL) security protocol for the TCP/IP (Internet) communication protocol. As should be clear from this description, it is important for the DAS to assure itself that a Transfer Agent is who the Agent purports to be. If not already provided in the course of signing an object, the Transfer Agent appends a hash, a cyclic redundancy check (CRC) information element, or other type of content integrity block to the object, thereby

Application Number 09/973, 273

ensuring the integrity, i.e., unchangeability, of the  
information object. [Emphasis mine]

Applicant respectfully traverses for the reasons put forth below and addressed below.

Bisbee does not disclose the authentication of an identity, or a signature, or a document using a videoconference.

Bisbee does not disclose a method of authenticating an individual or a signature or a document person to person. Bisbee discloses a method and system of using a transfer agent to witness the input of a digital signature; said transfer agent then relays the document to a third party through email or other means.

Bisbee does not disclose a method whereby the signatory to a document is authenticated by any other process than PKI. Rather, Bisbee discloses a method that authenticates that a document originated from a signatory (transfer agent), by using cryptography to identify the sender (transfer agent) of the document and cryptography to identify signed information objects within the document.

Bisbee does not disclose the use of a notary public to authenticate an identity, or a signature, or a document. The method of Bisbee is limited to the use of a

Application Number 09/973, 273

transfer agent who inputs a digital signature after witnessing data input into a document.

Bisbee does not disclose a method whereby the document to be authenticated by the authenticator (TCU) is created by the authenticator.

Paragraph 0028 of Bisbee states:

[0028] ... there is provided a method of handling stored e-original objects that have been created by signing information objects by respective Transfer Agents, submitting signed information objects to a TCU, validating the submitted signed information objects by at least testing the integrity of the contents of each signed information object and the validity of the signature of the respective Transfer Agent, and applying to each validated information object a date-time stamp and a digital signature and authentication certificate of the TCU. The method includes the steps selecting a stored e-original object; re-validating the selected e-original object by at least verifying the digital signature of the TCU applied to the selected e-original object; and applying to the re-validated e-original object a current date-time stamp and a digital signature and current authentication certificate of the TCU. [Emphasis mine]

The method of the pending application discloses a person to person authentication, using a videoconference. Bisbee discloses a method and system of authenticating that a document originated from a signatory; using cryptography to identify the sender (Transfer Agent) of the document.

Examiner states that Bisbee discloses a method of using a notary as a means to authenticate a document (line 1, page 7). Applicant respectfully traverses. Bisbee does not use a notary public as a means of authentication of an individual, a signature, or a document.

In fact , Bisbee is silent on the use of a “notary” as a means of authentication. Upon review of the Bisbee application, one will not find the term notary used as a means of authentication in the specification. In fact, Bisbee cites it's system and method as a substitute for document authentication when a notary public is not available.

Paragraph 0003 of Bisbee states:

[0003] The continuing evolution of the methods of commerce is evident in the increasing replacement of paper-based communications with electronic communications. When communication is by electronically

reproduced messages such as e-mail, facsimile machine, imaging, electronic data interchange or electronic fund transfer, however, there no longer exists a signature or seal to authenticate the identity of a party to a deal or transaction. The traditional legally accepted methods of verifying the identity of a document's originator, such as physical presence or appearance, a blue-ink signature, personal witness or Notary Public acknowledgment, are not possible. [Emphasis mine]

The Bisbee application further states in paragraph 0004:

[0004] To address these problems, a document authentication system (DAS) has been described that provides the needed security and protection of electronic information objects, or electronic documents and other information objects, and that advantageously utilizes an asymmetric cryptographic system to help ensure that a party originating an information object is electronically identifiable as such. .... [Emphasis mine]

Application Number 09/973, 273

The Bisbee patent fails to disclose the use of a “notary”, as traditionally understood in the legal sense of the word<sup>3</sup>:

Notary publics:

Etymology: Middle English notary clerk, notary public, from Latin notarius clerk, secretary, from noatarius of shorthand, from nota note, shorthand character.

: a public officer who attests or certifies writings (as a deed) to make them authentic and takes affidavits, depositions, and protests of negotiable paper—called also notary.

As paragraphs 3-4 of Bisbee depict, the method of Bisbee is to authenticate an electronic identity of an document when a notary is not available, using asymmetric cryptographic system as a means of authentication of a document. Bisbee fails to disclose any method, process, or system of notarization.

Bisbee fails to disclose a method whereby the third party authenticator (TCU) creates and issues the document being authenticated. Bisbee is premised on a transfer agent who witnesses a transaction whereby a document is digitally signed. The method of Bisbee teaches that the transfer agent conveys the document to the TCU. The TCU is not the originator of the document to be

---

<sup>3</sup> Merriam Webster Online Dictionary (<http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=notary+public&x=17&y=11>)

Application Number 09/973, 273

authenticated. The TCU is the recipient of the document of the document to be authenticated and functions as an after the fact authoritative custodian.

Paragraphs 0072-0073 of Bisbee disclose:

[0072] The TCU validates the Transfer Agent's identity and rights and verifies the integrity of submitted information objects. Use of digital signatures directly supports validation of both Transfer Agent identity and information object content integrity. Once it is determined that an information object has not been altered prior to or during submission and that the object's Transfer Agent has the proper authorizations, the TCU assumes custody and control of the object and responsibility for the object's preservation by appending a date-time stamp and digitally signing the submission. [Emphasis mine]

[0073] On receiving a digitally signed electronic object (block 114), the TCU tests the integrity of the electronic object's contents, the validity period of the Transfer Agent's certificate, and the status (valid or revoked) of the authentication certificate (e.g., ITU X.509v3 certificate(s)). The test of the integrity of the object contents, which may also be called "digital signature authentication", comprises



extracting the public key from the authentication certificate,  
decrypting the digital signature (thereby uncovering the  
object's hash), computing a new object hash, and checking  
the uncovered hash against the new hash. The test of the  
validity period comprises simply ensuring that the current  
date and time falls within the validity period noted in the  
certificate. The test of the validity of the certificate  
comprises querying the PKI to determine whether the  
certificate was not revoked or otherwise restricted at the  
time of digital signing. These three tests together may be  
called a "validation" process. Successful tests signify the  
authenticity of the received digitally signed electronic  
object, that is to say, who submitted the electronic object  
and that the object's contents have not changed during the  
submission process. [Emphasis mine]

The method of the present invention discloses that the third party authenticator (VVSC) creates and issues the document being authenticated, real-time. The method of Bisbee teaches that the transfer agent conveys the document to the TCU. The TCU is not the originator of the document to be authenticated. Likewise, there exists a serious lapse in the chain of custody of the document being authenticated.

Application Number 09/973, 273

Applicant submits that Bisbee fails to disclose a method whereby an identity or a signature or a document is authenticated during a real-time, live-stream videoconference, person to person. As such, Applicant submits that its method is not anticipated by Bisbee and is patentable over Bisbee.

Applicant submits that Bisbee fails to disclose a method whereby an identity or a signature or a document is authenticated during a real-time, live-stream videoconference using a notary public. As such, Applicant submits that its method is not anticipated by Bisbee is patentable over Bisbee.

Applicant submits that Bisbee fails to disclose a method whereby an identity or a signature or a document is authenticated during a real-time, live-stream videoconference, and whereby the authoritative document is created real-time.

As such, Applicant submits that its method is not anticipated by Bisbee is patentable over Bisbee.

Applicant submits that Bisbee fails to disclose a method whereby an identity or a signature or a document is authenticated during a real-time, live-stream videoconference and whereby the authoritative document is issued real-time. As such, Applicant submits that its method is not anticipated by Bisbee is patentable over Bisbee.

Applicant submits that with respect to Skarbo, the Examiner's objection be reconsidered in lieu of the foregoing analysis of Bisbee. Applicant further

Application Number 09/973, 273

submits that Skarbo fails to disclose a method of identity, or signature, or document authentication. Skarbo discloses a method of document collaboration.

### **DEPENDENT CLAIM OBJECTIONS**

Applicant respectfully submits that the foregoing arguments with respect to independent claims 1, 24 and 51 establish sufficient basis for the objections to be withdrawn and that the dependent claims be allowed (with the exception of the claims canceled by Applicant).

In reference to claims 2-23, these claims depend from independent claim 1, which Applicant believes to be allowable in view of the arguments above. As such, applicant submits that claims 2-23 are allowable by virtue of their dependence from claim 1.

In reference to claims 25-50, these claims depend from independent claim 24, which Applicant believes to be allowable in view of the arguments above. As such, applicant submits that claims 25-50 are allowable by virtue of their dependence from claim 24.

In reference to claims 52-77, these claims depend from it independent claim 51, which Applicant believes to be allowable in view of the arguments above. As such, applicant submits that claims 52-77 are allowable by virtue of their dependence from claim 51.

### **OTHER CITED REFERENCES**

The Examiner also cited other references on PTO form 892 but did not use these references in objection the claims. Applicant submits that because these references were not used to reject the claims, the additional references do not teach method of the pending application.

### **CONCLUSION**

Applicant submits that the stated grounds of rejection in the pending claims have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider and withdraw the presently outstanding rejections. It is believed that a full and complete response has been made to the outstanding office action, and as such, the amended application is in condition for allowance. Thus, prompt and favorable consideration of this amendment is respectfully requested. If the Examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at 310-739-9996 or 310-665-0111.

Respectfully Submitted,

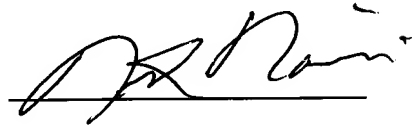
A handwritten signature in black ink, appearing to read 'Nick Nassiri', written over a horizontal line.

Nick Nassiri (Applicant/Inventor)

Application Number 09/973, 273

## DECLARATION

Applicant hereby submits a substitute specification, and replacement drawings and an oath stating that neither the substitute specification or replacement drawings contain any matter not included in the original specification or drawings.

A handwritten signature in black ink, appearing to read 'Nick Nassiri', is written over a horizontal line.

Nick Nassiri (Applicant/Inventor)